AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions of claims in the application:

Listing of Claims:

1. (Currently amended) A computer-implemented data security system that facilitates securing a data item, comprising:

a data store that includes at least one hierarchical data structure that comprises a plurality of data items; and

a security component that applies at least [[one]] a first security policy to at least a first subsection of the data store and at least a second variant security policy to at least a second disparate subsection of ~~to each of the plurality of data items within a defined region in~~ the data store.

2. (Original) The system of claim 1, the hierarchical data structure is at least one of a tree structure and a containment hierarchy.

3. (Original) The system of claim 2, the containment hierarchy is modeled as a Directed Acyclic Graph (DAG).

4. (Cancelled)

5. (Currently amended) The system of claim [[4]] 1, the at least first and second security ~~policy~~ policies [[is]] are at least one of mapped from within the data store and mapped from outside the data store.

6. (Currently amended) The system of claim 1, the at least first and second security ~~policy~~ policies [[is]] are at least one of explicitly mapped to an item and inherited by an item.

7. (Original) The system of claim 1, the security component includes an Access Control List having one or more Access Control Entries.

8. (Original) The system of claim 7, the Access Control List can be associated with a holding relationship of a containment hierarchy.

9. (Original) The system of claim 8, further comprising a plurality of Access Control Lists to facilitate security for the containment hierarchy.

10. (Original) The system of claim 1, the security component specifies a set of principals that are granted or denied access to perform operations on an item.

11. (Original) The system of claim 1, the security component includes at least one of discretionary access control list, a system access control list, and a security identifier.

12. (Original) The system of claim 1, further comprising an ordering component that arranges one or more Access Control Entries (ACE) in an Access Control List (ACL) to determine a security policy that is enforced for an item.

13. (Previously presented) The system of claim 12, further comprising the following ordering algorithm:

For inherited ACL's (L) on data item (I)
For items I1, I2
For ACE's A1 and A2 in L,
I1 is an ancestor of I2 and
I2 is an ancestor of I3 and
A1 is an ACE inherited from I1 and
A2 is an ACE inherited from I2
Implies
A2 precedes A1 in L,
wherein L and I are integers.

14. (Previously presented) The system of claim 12, further comprising the following ordering algorithm:

For inherited ACL's (L) on data item (I)

For items I1

For ACE's A1 and A2 in L,

I1 is an ancestor of I2 and

A1 is an ACCESS_DENIED_ACE inherited from I1 and

A2 is an ACCESS_GRANTED_ACE inherited from I1

Implies

A1 precedes A2 in L,

wherein L and I are integers.

15. (Previously presented) The system of claim 12, further comprising a component that evaluates access rights for a given principal to a given data item.

16. (Original) The system of claim 1, the security component further comprises an effective access control list that is obtained by processing lists inherited by an item and adding inheritable access control entries in an explicit access control list.

17. (Original) The system of claim 1, the security component further comprises an access mask specifying at least one of object-specific access rights, standard access rights, and generic access rights.

18. (Original) The system of claim 1, further comprising a security table for similarly protected security regions.

19. (Original) The system of claim 18, the security table includes at least one of the following fields an Item Identity, an Item Ordpath, an Explicit Item, a Path ACL, and a Region ACL.

20. (Previously presented) The system of claim 1, further comprising a component that does at least one of create a new item in a container, add an explicit ACL to an item, add a holding link to an item, delete a holding link from an item, delete an explicit ACL from an item and modify an ACL associated with an item.

21. (Original) A computer readable medium having computer readable instructions stored thereon for implementing the security component of claim 1.

22. (Currently amended) A computer-implemented method to facilitate data item security, comprising:

defining at least [[one]] first and second variant security ~~policy~~ policies for a data store that includes at least one hierarchical data structure containing a plurality of data items;

defining at least ~~one~~ first and second disparate security ~~region~~ regions for the data store including the at least one hierarchical data structure; and

applying the at least first security policy to the at least first security region and the at least second security policy to the at least second security region associated with the data store including the at least one hierarchical data structure.

23. (Original) The method of claim 22, further comprising automatically supporting at least one explicit and inherited security policy.

24. (Original) The method of claim 22, further comprising automatically ordering security policies.

25. (Original) The method of claim 22, further comprising processing security policies for at least one of a tree structure and a containment hierarchy.

26. (Original) The method of claim 22, further comprising mapping a security policy to a security region from a remote location from a database.

27. (Currently amended) The method of claim 22, the at least first and second security ~~policy~~ policies [[is]] are associated with an Access Control List having one or more Access Control Entries.

28. (Original) The method of claim 27, further comprising automatically arranging one or more Access Control Entries in the Access Control List to determine a security policy that is enforced for an item.

29. (Currently amended) A computer-implemented system that facilitates database security processing, comprising:

means for defining a first security policy and one or more disparate second security policies;

means for determining a first security region for the first security policy and one or more second security regions for the one or more second security policies; and

means for applying the first and one or more second security ~~policy~~ policies to a data store containing at least one of a tree structure and a containment hierarchy in accordance with the first and one or more second security ~~region~~ regions.

30. (Currently amended) A computer readable medium having a data structure stored thereon, comprising:

a first data field related to [[a]] at least first and second disparate security ~~region~~ regions associated with a data store containing at least one hierarchical data structure;

a second data field that relates to [[a]] at least first and second security ~~policy~~ policies; and

a third data field that links the at least first security policy to the at least first security region and the at least second security policy to the at least second security region.

31. (Original) The computer readable medium of claim 30, further comprising a field for an access mask specifying at least one of object-specific access rights, standard access rights, and generic access rights.

32. (Original) The computer readable medium of claim 30, further comprising a security field for similarly protected security regions.

33. (Previously presented) The computer readable medium of claim 32, the security field includes at least one of an Item Identity, an Item Ordpath, an Explicit Item, a Path ACL, and a Region ACL.